



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,985	04/01/2004	Michael O. Rabin	2645.2003-000	7288

21005 7590 01/18/2007  
HAMILTON, BROOK, SMITH & REYNOLDS, P.C.  
530 VIRGINIA ROAD  
P.O. BOX 9133  
CONCORD, MA 01742-9133

EXAMINER

AVERY, JEREMIAH L

ART UNIT PAPER NUMBER

2131

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/18/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

**Office Action Summary**

Application No.

10/815,985

Applicant(s)

RABIN ET AL.

Examiner

Jeremiah Avery

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 08 December 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-50 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-50 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 November 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. Claims 1-50 have been examined.
2. Responses to Applicant's Remarks have been given.

#### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-50 are rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent No. 7,043,636 to Smeets, hereinafter Smeets.

1. Regarding claim 1, Smeets teaches a method for creating a superfingerprint for identifying a software comprising:

executing said protected software at least once (column 3, lines 61-67, column 4, lines 1 and 2, "program instructions being executed by one or more processors", column 5, lines 13-22, "program code implementation", column 8, lines 40-60, "executing the program code 319 for the hash algorithm Hs" and column 9, lines 23-32, "program code implementation"); in each execution, using a supervising program, selecting specified portions of at least one of said executing software and of results of executing said protected software (column 3, lines 9-31, "dynamic

authorization data", column 5, lines 13-53, "portions of the static data", "portions of the dynamic data" and column 6, lines 19-61, "first dynamic audit hash value", "second dynamic audit hash value");

in each execution, using a supervising program, performing computations on said selected portions to obtain a collection of fingerprints (column 3, lines 25-31, "corresponding hash signature is then recomputed and stored back into the memory", column 5, lines 40-53, "audit hash value Ss is calculated by using a hash algorithm", column 6, lines 19-36, column 7, lines 14-26, "generate an expected value", column 8, lines 40-67, column 9, lines 1-22, 33-40 and 62-67 and column 10, lines 1-3 and 19-46);

combining, using the supervising program, said collections of fingerprints found in each execution into the superfingerprint of said protected software according to a combining rule (column 8, lines 40-60 and column 10, lines 4-46).

2. Regarding claim 2, Smeets teaches wherein the protected software is executed a plurality of times and the collection of fingerprints obtained during each execution are combined together according to the combining rule (column 3, lines 9-31 and "Different hash signatures are generated for the dynamic data object and the dynamic authorization data, respectively, and these are stored in the memory as well", "corresponding hash signature is then recomputed and stored back into memory as well" and lines 59-67, "sequences of actions to be performed by elements of a computer system", column 4, lines 1 and 2, column 5, lines 40-65, column 6, lines 1-53, "a unique

Art Unit: 2131

SerNo value", "two dynamic audit hash values are used", column 7, lines 7-13 and column 9, lines 11-22, "executed whenever it is desired").

3. Regarding claim 3, Smeets teaches wherein the combining rule outputs only those fingerprints that are computed in more than a specified number of executions (column 6, lines 19-61, "recomputed and stored back into non-volatile memory", column 7, lines 14-43, "a predetermined limit" and lines 66 and 67, column 8, lines 1-16 and 40-67, column 9, lines 1-22, "executed whenever it is desired", column 10, lines 19-31, "only if both of the tests are passed successfully" and lines 66 and 67 and column 11, lines 1-13).

4. Regarding claim 4, Smeets teaches wherein the combining rule removes from the output those fingerprints that occur in more than a specified number of executions of specified other protected softwares (column 6, lines 19-61, "recomputed and stored back into non-volatile memory", column 7, lines 14-43, "a predetermined limit" and lines 66 and 67, column 8, lines 1-16 and 40-67, column 9, lines 1-22, "executed whenever it is desired", column 10, lines 19-31, "only if both of the tests are passed successfully" and lines 66 and 67 and column 11, lines 1-13).

5. Regarding claim 5, Smeets teaches wherein fingerprints are not removed if they belong to a same group of protected software as said protected software (column 4, lines 36-62, column 6, lines 19-61, "recomputed and stored back into non-volatile memory", column 7, lines 14-32, "no modification will be permitted", column 8, lines 40-67 and column 9, lines 1-10)

Art Unit: 2131

6. Regarding claim 6, Smeets teaches wherein a fingerprint belongs to the superfingerprints of several protected softwares (column 3, lines 9-31 and "Different hash signatures are generated for the dynamic data object and the dynamic authorization data, respectively, and these are stored in the memory as well", "corresponding hash signature is then recomputed and stored back into memory as well" and lines 59-67, "sequences of actions to be performed by elements of a computer system", column 4, lines 1 and 2, column 5, lines 40-65, column 6, lines 1-53, "a unique SerNo value", "two dynamic audit hash values are used", column 7, lines 7-13 and column 9, lines 11-22).

7. Regarding claim 7, Smeets teaches storing in at least one data structure at least one fingerprint and means to identify said several protected softwares in whose superfingerprint said fingerprint is included (column 3, lines 9-31, "Different hash signatures are generated for the dynamic data object and the dynamic authorization data, respectively, and these are stored in the memory as well", "corresponding hash signature is then recomputed and stored back into memory as well" and lines 59-67, "sequences of actions to be performed by elements of a computer system", column 4, lines 1 and 2, column 5, lines 40-65, column 6, lines 1-53, "a unique SerNo value", "two dynamic audit hash values are used", column 7, lines 7-13 and column 9, lines 11-22).

8. Regarding claim 8, Smeets teaches wherein the means to identify is a bit vector data structure whose  $m$ th bit indicates whether the superfingerprint associated with the  $m$ th member of said several protected softwares includes said fingerprint (column 3, lines 9-31, "dynamic data structure" and 59-67 and column 4, lines 1-15 and 39-62).

Art Unit: 2131

9. Regarding claim 9, Smeets teaches wherein associated with each said fingerprint there are at least two numbers  $k_1$  and  $k_2$  where  $k_2$  is greater than or equal to  $k_1$  that indicate that the fingerprints of protected softwares from  $k_1$  to  $k_2$  of said several protected softwares all include said fingerprint (column 6, lines 19-53, "first dynamic audit hash value", "second dynamic audit hash value", "different input parameters", "two distinctly different audit has values", column 8, lines 40-60 and column 10, lines 4-18).

10. Regarding claim 10, Smeets teaches wherein said several protected softwares belong to a group of protected software (column 5, lines 13-53, "portions of the static data that are attributable to system-defined parameters", "portions of the dynamic data that are attributable to system-defined parameters").

11. Regarding claim 11, Smeets teaches wherein the fingerprints of various protected softwares are stored in a data structure to facilitate and accelerate retrieval of fingerprints and associated names of protected software (column 6, lines 19-53, "recomputed and stored back into non-volatile memory", column 7, lines 14-26, column 8, lines 1-16 and 40-60 and column 9, lines 7-40, "stored in the IROM", "EEPROM").

12. Regarding claim 12, Smeets teaches wherein the executing protected software is partitioned into pages, said specified portions are selected from said pages and the computations produce a fingerprint for each portion (column 3, lines 59-67, column 4, lines 1-35, column 5, lines 13-39, column 8, lines 40-60 and column 9, lines 11-40, "program code implementation").

13. Regarding claim 13, Smeets teaches wherein said specified portions are selected from the protected software stored in a memory of the device executing said

Art Unit: 2131

protected software (column 3, lines 59-67, column 4, lines 1-35, column 5, lines 13-39, column 8, lines 40-60 and column 9, lines 11-40, "program code implementation").

14. Regarding claim 14, Smeets teaches wherein said specified portions are selected from the protected software stored in secondary memory of the device executing said protected software (column 3, lines 59-67, column 4, lines 1-35, column 5, lines 13-39, "protect those portions of the static data that are attributable to system-defined parameters", column 6, lines 19-53, "first dynamic audit hash value", "second dynamic audit hash value", column 8, lines 40-60 and column 9, lines 11-40, "program code implementation").

15. Regarding claim 15, Smeets teaches wherein the specified portions are basic blocks of programs (column 3, lines 59-67, column 4, lines 1-35, column 5, lines 13-39, "protect those portions of the static data that are attributable to system-defined parameters", column 6, lines 19-53, "first dynamic audit hash value", "second dynamic audit hash value", column 8, lines 40-60 and column 9, lines 11-40, "program code implementation").

16. Regarding claim 16, Smeets teaches wherein the computation involves only parts of said selected portions (column 3, lines 59-67, column 4, lines 1-35, column 5, lines 13-39, "protect those portions of the static data that are attributable to system-defined parameters", column 6, lines 19-53, "first dynamic audit hash value", "second dynamic audit hash value", column 8, lines 40-60 and column 9, lines 11-40, "program code implementation").



Art Unit: 2131

17. Regarding claim 17, Smeets teaches wherein said involved parts are operation codes (column 3, lines 59-67, column 4, lines 1-35, column 5, lines 13-39, "protect those portions of the static data that are attributable to system-defined parameters", column 6, lines 19-53, "first dynamic audit hash value", "second dynamic audit hash value", column 8, lines 40-60 and column 9, lines 11-40, "program code implementation").

18. Regarding claim 18, Smeets teaches wherein said involved parts are information in an audio signal (column 3, lines 59-67 and column 4, lines 1-15, "audio frequency").

19. Regarding claim 19, Smeets teaches wherein said involved parts are information in a visual display (column 1, lines 46-61, "personal digital assistants (PDAs) and cellular telephones").

[It is known in the art that PDAs and cellular telephones possess visual display capabilities.]

20. Regarding claim 20, Smeets teaches wherein the selected portion concerns the interaction between at least one user and the execution of protected software (column 3, lines 59-67, column 4, lines 1-62, "the user is required to correctly supply an access code in order to be permitted to modify the dynamic data", column 5, lines 13-39, "protect those portions of the static data that are attributable to system-defined parameters", column 6, lines 19-53, "first dynamic audit hash value", "second dynamic audit hash value", column 8, lines 40-60 and column 9, lines 11-40, "program code implementation").

Art Unit: 2131

21. Regarding claim 21, Smeets teaches wherein the output to the computation is a sequence (column 1, lines 47-65, "International Mobile Equipment Identity (IMEI) number").

[As it is known in the art, an IMEI number is a 15-digit serial number on each phone that can normally be found behind the battery in the phone and can be revealed by entering a key command. When that occurs, the visual display will output the sequence of 15 digits that comprise the IMEI number.]

22. Regarding claim 22, Smeets teaches wherein the computation is a hash function value of said portion (column 3, lines 59-67, column 4, lines 1-35, column 5, lines 13-39, "protect those portions of the static data that are attributable to system-defined parameters", column 6, lines 19-53, "first dynamic audit hash value", "second dynamic audit hash value", column 8, lines 40-60 and column 9, lines 11-40, "program code implementation").

23. Regarding claim 23, Smeets teaches wherein the hash function value is computed by polynomial fingerprinting (column 3, lines 59-67, column 4, lines 1-35, column 5, lines 13-39, "protect those portions of the static data that are attributable to system-defined parameters", column 6, lines 19-53, "first dynamic audit hash value", "second dynamic audit hash value", column 8, lines 40-60 and column 9, lines 11-40, "program code implementation").

24. Regarding claim 24, Smeets teaches wherein the computation is a computation on an audio signal (column 3, lines 59-67 and column 4, lines 1-15, "audio frequency").

Art Unit: 2131

25. Regarding claim 25, Smeets teaches wherein the computation is a computation on a video stream (column 1, lines 46-61, "personal digital assistants (PDAs) and cellular telephones").

[It is known in the art that PDAs and cellular telephones possess visual display capabilities.]

26. Regarding claim 26, Smeets teaches a method for identifying a first protected software comprising the steps of:

storing previously created superfingerprints for at least one protected software (column 3, lines 9-31, "Different hash signatures are generated for the dynamic data object and the dynamic authorization data, respectively, and these are stored in the memory as well", "corresponding hash signature is then recomputed and stored back into memory as well" and lines 59-67, "sequences of actions to be performed by elements of a computer system", column 4, lines 1 and 2, column 5, lines 40-65, column 6, lines 1-53, "a unique SerNo value", "two dynamic audit hash values are used", column 7, lines 7-13 and column 9, lines 11-22);

executing said first protected software at least once;

selecting specified portions of at least one of said executing protected software and of the results of executing said protected first software on each execution (column 3, lines 61-67, column 4, lines 1 and 2, "program instructions being executed by one or more processors", column 5, lines 13-22, "program code implementation", column 8, lines 40-60, "executing

the program code 319 for the hash algorithm Hs" and column 9, lines 23-32, "program code implementation");

performing specified computations on said selected portions to obtain a collection of fingerprints (column 3, lines 25-31, "corresponding hash signature is then recomputed and stored back into the memory", column 5, lines 40-53, "audit hash value Ss is calculated by using a hash algorithm", column 6, lines 19-36, column 7, lines 14-26, "generate an expected value", column 8, lines 40-67, column 9, lines 1-22, 33-40 and 62-67 and column 10, lines 1-3 and 19-46);

comparing said collection of fingerprints to said previously computed superfingerprint of at least one second protected software to determine whether there is an approximate match (column 3, lines 25-31 and column 7, lines 14-32);

declaring said first software to be the same as said second protected software if an approximate match is found (column 3, lines 25-31 and column 7, lines 14-32).

27. Regarding claim 27, Smeets teaches wherein said specified portions of said executing protected software and of said results of executing said software, are stored in a memory of a device executing said software (column 6, lines 19-53, "recomputed and stored back into non-volatile memory", column 7, lines 14-26, column 8, lines 1-16 and 40-60 and column 9, lines 7-40, "stored in the IROM", "EEPROM").

Art Unit: 2131

28. Regarding claim 28, Smeets teaches wherein said specified portions of at least one of said executing protected software and of said results of executing said protected software, are selected from recently accessed portions of the protected software stored in the memory of the device executing said protected first software (column 3, lines 9-31, "dynamic authorization data", column 5, lines 13-53, "portions of the static data", "portions of the dynamic data" and column 6, lines 19-61, "first dynamic audit hash value", "second dynamic audit hash value").

29. Regarding claim 29, Smeets teaches wherein said specified components of said executing protected software are selected from portions of said executing protected software stored in secondary storage (column 6, lines 19-53, "recomputed and stored back into non-volatile memory", column 7, lines 14-26, column 8, lines 1-16 and 40-60 and column 9, lines 7-40, "stored in the IROM", "EEPROM").

30. Regarding claim 30, Smeets teaches wherein the portions of said executing protected software are selected while said protected software is sent from one device to another (column 1, lines 47-65, column 2, lines 59-67 and column 4, lines 1-15).

31. Regarding claim 31, Smeets teaches wherein said portions of the results of execution of said protected software are selected from the output of the device executing said protected software (column 3, lines 9-31, "dynamic authorization data", column 5, lines 13-53, "portions of the static data", "portions of the dynamic data" and column 6, lines 19-61, "first dynamic audit hash value", "second dynamic audit hash value").

32. Regarding claim 32, Smeets teaches wherein said specified portions of at least one of said executing protected software and of the results of executing said protected software on a later execution are dependent on the results of an earlier approximate match (column 3, lines 25-31 and column 7, lines 14-32).

33. Regarding claim 33, Smeets teaches wherein determining the approximate match comprises:

determining whether the amount of said commonality between fingerprints of said first protected software and the fingerprints comprising said superfingerprint of said at least one second protected software exceeds a specified threshold in which case the first protected software is identified to be the same as the second protected software (column 3, lines 25-31 and column 7, lines 14-43).

34. Regarding claim 34, Smeets teaches wherein said specified threshold is exceeded only if the amount of commonality between said fingerprints of said first protected software and the fingerprints comprising said superfingerprint of said second protected software exceed the commonality between said fingerprints of said first protected software and the fingerprints comprising the superfingerprint of a third protected software (column 3, lines 25-31 and column 7, lines 14-43).

35. Regarding claim 35, Smeets teaches wherein the commonality between the fingerprints of said first protected software and said second protected software depends on the number of fingerprints that are the same in said two protected softwares with a weighting factor for each equal fingerprint (column 3, lines 25-31 and column 7, lines 14-43).

36. Regarding claim 36, Smeets teaches wherein commonality further depends on the number of fingerprints that are different in said two protected softwares with a weighting factor for each unequal fingerprint (column 3, lines 25-31 and column 7, lines 14-43).

37. Regarding claim 37, Smeets teaches wherein commonality further depends on the relative positions of the portions of protected software from which at least two fingerprints are computed (column 3, lines 25-31, "corresponding hash signature is then recomputed and stored back into the memory", column 5, lines 40-53, "audit hash value Ss is calculated by using a hash algorithm", column 6, lines 19-36, column 7, lines 14-26, "generate an expected value", column 8, lines 40-67, column 9, lines 1-22, 33-40 and 62-67 and column 10, lines 1-3 and 19-46).

38. Regarding claim 38, Smeets teaches wherein the specified computation involves only parts of said selected portions (column 3, lines 59-67, column 4, lines 1-35, column 5, lines 13-39, "protect those portions of the static data that are attributable to system-defined parameters", column 6, lines 19-53, "first dynamic audit hash value", "second dynamic audit hash value", column 8, lines 40-60 and column 9, lines 11-40, "program code implementation").

39. Regarding claim 39, Smeets teaches wherein said involved parts are operation codes (column 3, lines 59-67, column 4, lines 1-35, column 5, lines 13-39, "protect those portions of the static data that are attributable to system-defined parameters", column 6, lines 19-53, "first dynamic audit hash value", "second dynamic audit hash

Art Unit: 2131

value", column 8, lines 40-60 and column 9, lines 11-40, "program code implementation").

40. Regarding claim 40, Smeets teaches wherein said involved parts are information in an audio signal (column 3, lines 59-67 and column 4, lines 1-15, "audio frequency").

41. Regarding claim 41, Smeets teaches wherein said involved parts are information in a visual display (column 1, lines 46-61, "personal digital assistants (PDAs) and cellular telephones").

[It is known in the art that PDAs and cellular telephones possess visual display capabilities.]

42. Regarding claim 42, Smeets teaches wherein the selected portion concerns the interaction between at least one user and the execution of protected software (column 3, lines 59-67, column 4, lines 1-62, "the user is required to correctly supply an access code in order to be permitted to modify the dynamic data", column 5, lines 13-39, "protect those portions of the static data that are attributable to system-defined parameters", column 6, lines 19-53, "first dynamic audit hash value", "second dynamic audit hash value", column 8, lines 40-60 and column 9, lines 11-40, "program code implementation").

43. Regarding claim 43, Smeets teaches wherein the input to the computation is a sequence (column 4, lines 36-62, "access code itself is a string of randomly chosen symbols" and column 10, lines 4-46)

44. Regarding claim 44, Smeets teaches wherein the input to the comparison is a collection of fingerprints each having an associated weight (column 5, lines 40-65,



Art Unit: 2131

"associate a static audit hash value, or signature" and column 6, lines 19-61, "two distinctly different audit hash values").

45. Regarding claim 45, Smeets teaches wherein the computation is a hash function value of said portion (column 3, lines 25-31, "corresponding hash signature is then recomputed and stored back into the memory", column 5, lines 40-53, "audit hash value Ss is calculated by using a hash algorithm", column 6, lines 19-36, column 7, lines 14-26, "generate an expected value", column 8, lines 40-67, column 9, lines 1-22, 33-40 and 62-67 and column 10, lines 1-3 and 19-46).

46. Regarding claim 46, Smeets teaches wherein the hash function value is computed by polynomial fingerprinting (column 3, lines 25-31, "corresponding hash signature is then recomputed and stored back into the memory", column 5, lines 40-53, "audit hash value Ss is calculated by using a hash algorithm", column 6, lines 19-36, column 7, lines 14-26, "generate an expected value", column 8, lines 40-67, column 9, lines 1-22, 33-40 and 62-67 and column 10, lines 1-3 and 19-46).

47. Regarding claim 47, Smeets teaches wherein the computation is a computation of an audio signal (column 3, lines 59-67 and column 4, lines 1-15, "audio frequency").

48. Regarding claim 48, Smeets teaches wherein the computation is a computation of a video stream (column 1, lines 46-61, "personal digital assistants (PDAs) and cellular telephones").

[It is known in the art that PDAs and cellular telephones possess visual display capabilities.]

Art Unit: 2131

49. Regarding claim 49, Smeets teaches a method for identifying a protected software group of a first software comprising the steps of:

storing previously created superfingerprints for at least one protected software group (column 3, lines 9-31, "Different hash signatures are generated for the dynamic data object and the dynamic authorization data, respectively, and these are stored in the memory as well", "corresponding hash signature is then recomputed and stored back into memory as well" and lines 59-67, "sequences of actions to be performed by elements of a computer system", column 4, lines 1 and 2, column 5, lines 40-65, column 6, lines 1-53, "a unique SerNo value", "two dynamic audit hash values are used", column 7, lines 7-13 and column 9, lines 11-22);

executing said first protected software at least once (column 3, lines 61-67, column 4, lines 1 and 2, "program instructions being executed by one or more processors", column 5, lines 13-22, "program code implementation", column 8, lines 40-60, "executing the program code 319 for the hash algorithm Hs" and column 9, lines 23-32, "program code implementation");

selecting specified portions of said executing first protected software and of the results of executing said first protected software on each execution (column 3, lines 9-31, "dynamic authorization data", column 5, lines 13-53, "portions of the static data", "portions of the dynamic data" and column 6,

lines 19-61, "first dynamic audit hash value", "second dynamic audit hash value");

performing specified computations on said selected portions to obtain a collection of fingerprints (column 3, lines 25-31, "corresponding hash signature is then recomputed and stored back into the memory", column 5, lines 40-53, "audit hash value Ss is calculated by using a hash algorithm", column 6, lines 19-36, column 7, lines 14-26, "generate an expected value", column 8, lines 40-67, column 9, lines 1-22, 33-40 and 62-67 and column 10, lines 1-3 and 19-46);

comparing said collection of fingerprints to said previously computed superfingerprint of at least one second protected software group to determine whether there is an approximate match (column 3, lines 25-31 and column 7, lines 14-32);

declaring said first protected software to be a member of said second protected software group if an approximate match is found (column 3, lines 25-31 and column 7, lines 14-32).

50. Regarding claim 50, Smeets teaches a method for identifying a protected software that is a member of a group of protected software comprising the steps of:

storing previously created superfingerprints for at least one protected software group and for members of that group (column 3, lines 9-31, "Different hash signatures are generated for the dynamic data object and the dynamic authorization data, respectively, and these are stored in the

memory as well", "corresponding hash signature is then recomputed and stored back into memory as well" and lines 59-67, "sequences of actions to be performed by elements of a computer system", column 4, lines 1 and 2, column 5, lines 40-65, column 6, lines 1-53, "a unique SerNo value", "two dynamic audit hash values are used", column 7, lines 7-13 and column 9, lines 11-22);

executing said protected software at least once (column 3, lines 61-67, column 4, lines 1 and 2, "program instructions being executed by one or more processors", column 5, lines 13-22, "program code implementation", column 8, lines 40-60, "executing the program code 319 for the hash algorithm Hs" and column 9, lines 23-32, "program code implementation"); selecting specified portions of said executing protected software and of the results of executing said protected software on each execution (column 3, lines 9-31, "dynamic authorization data", column 5, lines 13-53, "portions of the static data", "portions of the dynamic data" and column 6, lines 19-61, "first dynamic audit hash value", "second dynamic audit hash value");

performing computations on said selected portions to obtain a collection of fingerprints (column 3, lines 25-31, "corresponding hash signature is then recomputed and stored back into the memory", column 5, lines 40-53, "audit hash value Ss is calculated by using a hash algorithm", column 6, lines 19-36, column 7, lines 14-26, "generate an expected value", column

8, lines 40-67, column 9, lines 1-22, 33-40 and 62-67 and column 10, lines 1-3 and 19-46);

comparing said collection of fingerprints to said previously computed superfingerprint of at least one second protected software group and the superfingerprints of the members of said second protected software group to determine whether there is an approximate match with said group and at least one of said superfingerprints of said members of said group (column 3, lines 25-31 and column 7, lines 14-32);

declaring said protected software to be the same as a particular member of said second protected software group if an approximate match is found (column 3, lines 25-31 and column 7, lines 14-32).

### ***Response to Arguments***

51. Applicant's arguments filed 12/08/06 have been fully considered but they are not persuasive. With regards to claim 1, the Examiner maintains that Smeets discloses the claimed invention, as cited above. Pertaining to the "executing said protected software at least once", the Examiner maintains the above-cited grounds of rejection, in particular but not limited to, column 5, lines 13-22, "program code implementation" and column 8, lines 40-60, "executing the program code 319 for the hash algorithm Hs".

52. In regards to the "fingerprints" as claimed by the Applicant, the Examiner maintains the above-cited grounds of rejection. It is known in the art that a hash value is used as a "fingerprint" for a file, which can be used to detect changes in the file.

Thus, the disclosure of hash values by Smeets discloses the fingerprints as claimed by the applicant.

53. Pertaining to the "selected portions", the Examiner maintains that the "portions of the static data" and the "portions of the static data", as well as "the stored data is checked by the processing circuits 300 by computing at given *controlled instants* an expected second dynamic audit hash value" disclosed by Smeets disclose the claimed invention.

54. With regards to Claim 2, pertaining to the "executing the protected software a plurality of times", the Examiner maintains that Smeets discloses this. The Examiner refers to the above-cited grounds of rejection, in particular, but not limited to, column 9, lines 11-22, "the program code 319 for the static hash algorithm Hs is executed whenever it is desired".

55. Also, with regards to "identifying a protected software that is a member of a group of protected software" as claimed in claim 50, the Examiner maintains the above cited grounds of rejection, in particular but not limited to column 6, lines 1-53, " each realization of a system is given a unique SerNo value. In alternative embodiments, limited numbers of realizations of a system may be assigned the same SerNo value". With the "same SerNo value" being assigned to more than one particular component, it is broadly interpreted by the Examiner that said "limited number of realizations" belong to a group since they would each possess said "same SerNo value".

***Conclusion***

56. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

57. The following United States Patents are cited to further show the state of the art with respect to the secure identification of software, such as:

United States Patent No. 6,165,072 to Davis et al., which is cited to show verifying communications over a network.

United States Patent No. 5,933,498 to Schneck et al., which is cited to show a system for controlling access and distribution of digital property.

United States Patent No. 5,646,997 to Barton which is cited to show a method and apparatus for embedding authentication information within digital data.

United States Patent No. 5,926,624 to Katz et al., which is cited to show employing authentication and encryption protocols for the secure transfer of digital information:

United States Patent No. 6,170,060 to Mott et al., which is cited to show embedding identification information within a file and only playing said file if the ID matches that of the playback device.

United States Patent No. 6,122,403 to Rhoads, which is cited to show a computer system linked by using information in data objects.

58. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

59. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.


60. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeremiah Avery whose telephone number is (571) 272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

61. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



62. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JLA

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100